Asian Journal of Information Technology 16 (9): 716-721, 2017
ISSN: 1682-3915

Proposed Multi-Level Security Depended on Steganography and Modified Cryptography

Fadhil Salman Abed
Department of Information Technology, Sulaimani Polytechnic University,
Kurdistan, Khanaqeen, Iraq

Abstract: A new technique proposed with the combination of steganography and cryptography enhanced with new secure feature for generating a new security system. Cryptography and steganography are two popular ways for secure data transmission in which the former distorts a message, so it cannot be understood and another hides a message, so it cannot be seen. In this study, a new digital message hiding system is proposed for the combination of steganography based on fractal image compression and modified RSA with Diffe-Hellman. The combination of these two techniques satisfies the requirements such as highly security and robustness between sender and receiver. The proposed method ensures acceptable image quality with very little distortion in the image. The main advantage of this system is that, the method used for modified RSA depended on multi-prime with Diffe-Hellman algorithm which is very secure and the fractal transformation technique is very hard to detect in image steganography. It also produces efficient robustness of stego-image though, it had been attacked by other techniques and additionally saved from attacks. Goal of this study is to develop a new security system that messages cannot be retrieved easily from the image by any attackers or hackers in the communication process.

Key words: Image processing, hiding, fractal image compression, quadtree, steganography, public key cryptosystem, RSA, N-prime RSA security, private key

INTRODUCTION

In networking, cryptography can be specified as the security service for data and telecommunications. Cryptography is an important way to address message transmission security requirements. Encryption and decryption of messages are made for the technique of cryptography (Shereek *et al*., 2014). A mechanism of hiding the original messages from the intruders and by making a suspect of the existence of the message only to the intended receiver is called steganography. Here, the secret message is sent as image or text through the encryption of the message in which special keys are arranged for those intended receivers to get the original message. The receiver only makes actual procedure of the real message sent by the sender. Real message can be letters or digits which can be encrypted as hidden message in any form as audio or video or image (Anderson and Petitcolas, 1998). Steganography must not be confused with cryptography where the message is transformed, so as to make its meaningless to malicious people who intercept it. The goal of steganography is to avoid drawing suspicion to the transmission of the secret message between sender and receiver. A secure data transmission is made using cryptography and steganography. Combination of both these two techniques results in appearing a highly secured method for data communication (Juneja and Sandhu, 2013).

THE PRPOSED HIDING SYSTEM

The proposed algorithm is based on our fractal encoding method and the hybrid modified RSA with Diffie Hellman algorithm for encryption. In this an image file is taken for embedding the secret text. Both files are converted in binary equivalent. A XOR operation is applied on embedding process to make the method more secure. The text is embedded using the Fractal Encoding method algorithm and this encrypted text by modified RSA . The embedded image file is called as stego image, Fig. 1 illustrated the proposed system.

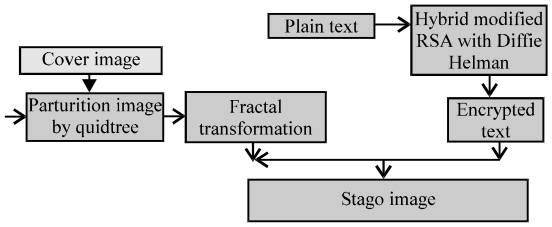

Fig. 1: Block diagram of the proposed hybrid system

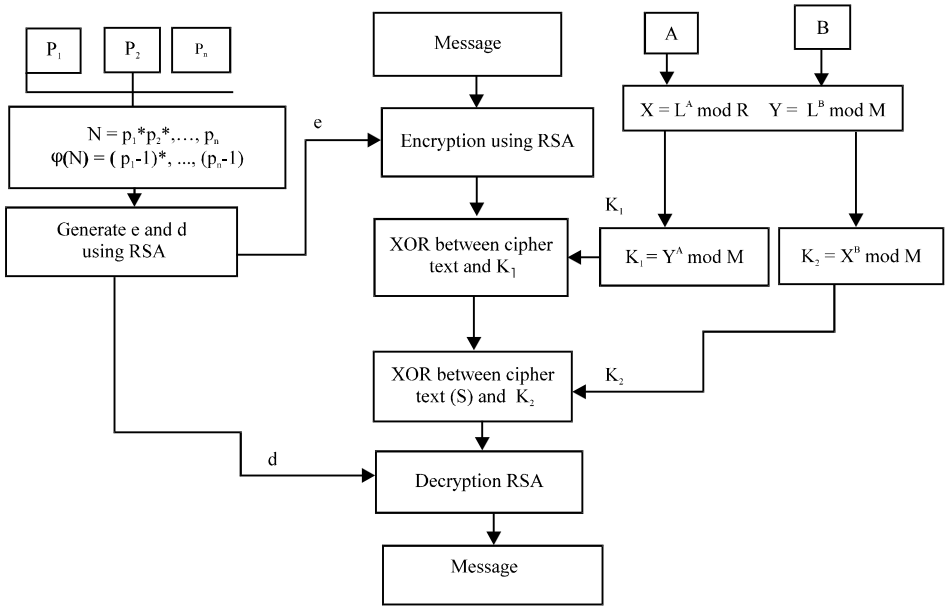

Fig. 2: Block diagram of the proposed hybrid modified RSA with Diffie-Hellman

Hybrid modified RSA with Diff-Hellman: In current techniques everything is being transferred on the internet and other communication medium. So that, we need to make our data more secure from all other attacker and unauthorized person. So that, we have to give lot of protection schemes to the transmitting data. For that, we have lots of cryptography methods.

But most of cryptography methods keep need to modified the level of security under development of technology and counter-technology. So, that with reference to the RSA and other famous algorithms as Diffie Hellman and N-prime RSA, Fig. 2 and Algorithm 1 with example illustrated the modified system.

Algorithm 1; The proposed hybrid modified RSA with Diffie-Hellman:

Step 1: Chose the public-key for Diffie Hellman system
Key generation:
Choose two random number A, B and L, M where L chose one of primitive roots of M
Now calculate following as public number:
$X = L^A \bmod M$, $Y = L^B \bmod M$

Step 2: Chose the Public-Key for modified RSA stage system
Key generation:
Let N be the product of r, randomly chosen distinct primes $N = p_1 * p_2, ..., *p_r$
Compute Euler's Totient function of N:
$\varphi(N) = \Pi_{i=1}{}^{r}(p_i-1)$
Choose an integer e, $1<e<\varphi\ \sigma(N)$ such that gcd(e, φ(N)) = 1
the pair (N, e) is the public key

Step 3: Secrete key calculation (Diffie Hellman method)
$K_1 = Y^A \bmod M$, $K_2 = X^B \bmod M$

Step 4: Secrete key calculation (RSA method)
Compute the integer d€ZN such that ed = 1 mod φ(N), here, d is the private key, the pair $(p_1, p_2, ..., p_r, e)$ is the secrete key

Step 5: Encryption:
Encrypt message using RSA algorithm
$C_1 = (Msg^e) \bmod N$
Doing X-OR between C_1 and key K_1

$S = C_1 \oplus K_1$

Step 6: Decryption:
At receiver side X-OR is between S and K_e

Algorithm 2; Test the proposed hybrid modified RSA with Diffie-Hellman:

Step 1: Chose the public-key for Diffie Hellman system
Key generation:
Choose random number A = 5, B = 6 and L = 2, M = 177 where, L chose one of primitive roots of 177
Now calculate following as public number:
$X = 2^5 \bmod 177 = 32$, $Y = 2^6 \bmod 177 = 64$

Step 2: Chose the public-key for modified RSA stage system
Key generation:
Let N be the product of r, randomly chosen distinct primes $N = p_1 * p_2, ..., *p_r = 2\times3\times5\times7\times11\times13 = 30030$
Compute Euler's Totient function of N:
$\sigma(N) = 1\times2\times4\times6\times10\times12 = 5760$
Choose an integer e(public-key) such is not factor of 5760
$5760 = 2\times2\times2\times2\times2\times2\times2\times3\times5$, e = 7 or 11 or 13, assume e = 7

Step 3: Secrete key calculation (Diffie Hellman method)

$K_1 = Y^A \bmod R = 32^6 \bmod 177 = 175$, $K_2 = X^B \bmod R = 64^5 \bmod 177 = 175$

Step 4: Secrete key calculation (RSA method)
$D = e^{-1} \bmod \varphi(N) = 7^{-1} \bmod 5760 = 823$

Step 5: Encryption(Assume the message "2"
Encrypt message using RSA algorithm
$C_1 = (Msg^e) \bmod N = 2^7 \bmod 30030 = 128$
Doing X-OR between C_1 and key K_1
$S = C1 \oplus K_1 = 128 \oplus 175 = 47$

Step 6: Decryption:
At receiver side X-OR is between S and key K_2

Quad-tree partition: There are various kinds of partitioning methods to compartmentalize ranges. For example, block-based partition, quad-tree partition, HV partition and Triangular partition. In this research, we implement quad tree partition. The quad tree partition employs the well known image processing technique based on a recursive splitting of selected image quadrants, enabling the resulting partition to be represented by a tree structure in which each non terminal node has four descendants. The partition is constructed by selecting an initial level in the tree (corresponding to some maximum range block size) and recursively partitioning any block for which a match better than some preselected threshold is not found. In a quad tree partition, a square in the image is broken up into 4 equally sized sub squares when it is not covered well enough by a domain (Cheng *et al*., 2001; Schettini, 1993; Fisher, 1995).

Fractal image transformation: There are two general categories of compression methods-lossless and lossy methods. A lossless method will produce an image that when decompressed is identical to the original image down to the last bit Table 1. A lossy method on the other hand will produce an image that closely resembles but is not an exact duplicate of the original image. The major drawback of lossless methods is that they cannot achieve very high compression ratios (usually about 2-1). Hence, for image compression applications where the input files are usually measured in megabytes and where the losses of very minor graphic details are not critical, lossy methods are mostly used (Fisher, 1995; Shanyu and Yongfeng, 2011). For certain applications such as the compression of text files or executable codes, lossless compression is a necessity, of course. Figure 3 illustrated the main steps of fractal image encoding.

Fractal image compression: For each range block R the optimal affine approximation (mapping) can be represented as Keerthika (207) and Kaur and Kaur (2017):

$$R_i \approx sD_i + o \quad (1)$$

Where:
R_i = The Range pixel value
D_i = The corresponding Domain pixel value
s = The scaling coefficient
o = The offset coefficient

Information extraction: After the data file (stego-image) has been loaded, the process of reconstructing SecData is applied to extract the array of embedded secret characters which have been stored in the (IFS) coefficients (s, o) in a reverse way. This stage implies the following steps: extract the two digit of the fraction part of the coefficient (s and o) with keeping the integer part:

Table 1: Fractal image compression

No.	Symmetric
1	Identity
2	Rotation (+90)
3	Rotation (+180)
4	Rotation (+270)
5	Reflection about mid-vertical axis
6	Reflection and rotation (-90)
7	Reflection and rotation (-180)
8	Reflection and rotation (-270)

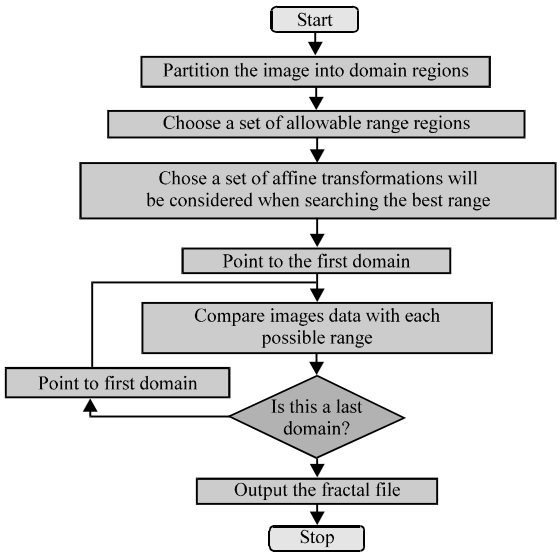

Fig. 3: Fractal image compression

$$V = IFS(I) \times scl - Fix(IFS(I) \times scl)$$
$$Vs = v \times 1oo$$

Convert the extracted data to byte:

$$SecData(I) = CByte((Vs - Fix(Vs)) \times 1000$$

Convert the bytes to string representation:

$$recSecData = recSecData \text{ and } Cstr(Chr(SecData(I)))$$

Display the secret message: Fractal encoding searching for similarity is performed between the range and the domain blocks and the information is stored in an index, then the image (cover-image) information is stored as a structure array of data containing the secret message (Fig. 4).

Fractal decoding: The goal of this system is to embed or hide information (text, numbers, symbols or equations) in a cover-image (BMP format) after compressing the image to produce the stego-image as a data file. System implementation accepts six inputs in the embedding stage:

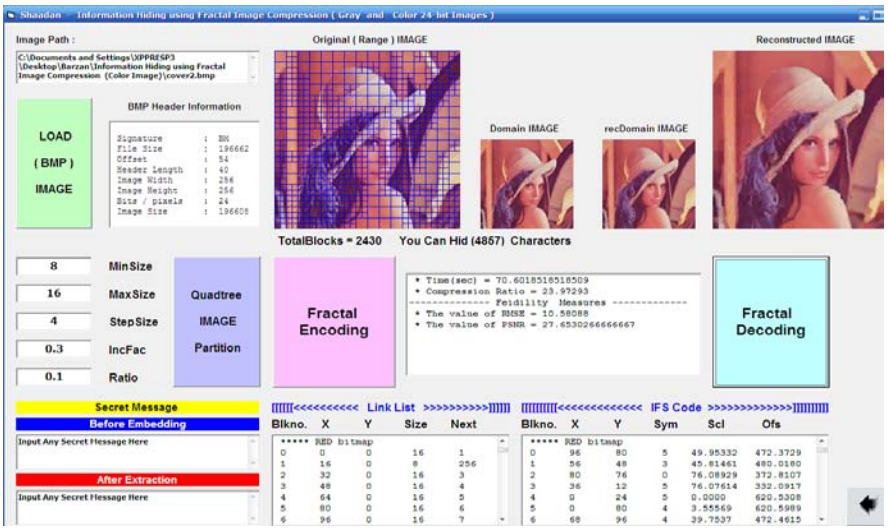

Fig. 4: Fractal encoded data

- Loading the cover image (BMP.format) as the input file
- Input control parameters
- Quad-tree partitioning the colour component
- Domain generating
- Inputting the secret message for embedding
- Fractal encoding which include embedding

The received data is a collection of data that represent the image with the secret message. The receiver will extract the embedded information (secret message) and then reconstruct the cover image. Setting the value of partitioning control parameters:

- The maximum block size (SizMax)
- The minimum block siz (SizMin)
- Inclusion factor is the multiple factor when it is multiplied by the global standard deviation (σ), it will define the value of the desperation threshold (Eσ) and If>0:

$$E\sigma = If \times \sigma$$

Acceptance ratio (Ar) is the ratio of the number of pixels whose value differs from the block mean by a distance more than desperation threshold (Eσ). As the value of the acceptance ratio is selected small then in all regions of the image which have a significant degree of contrast will partition into small blocks and therefore, a higher image (Fig. 5).

The effect of hiding secret message: The main objective of the proposed system of hiding and encryption is to embed a secret message with a huge number of characters as possible with different images and numbers without degrading the quality of the reconstructed cover image. So, to evaluate the effect of the secret message embedding on the cover image, a set of tests is applied. Table 2 show, the result of hiding and encryption different message process.

Table 2: Hiding effect on different images

Images (256×256)	No. block (by using quad-tree partition)	No. characters (Length of secret message (SecData) = (No. of blocks ×2) $^{-3}$)	Time (sec)	PSNR
	7926	15849	110.53	31.064
	11406	22809	120.4	30.01
	5220	10455	105.3	29.4
	4941	9879	99.5	30.8

Minimum block size = 4; Maximum block size = 8 Step size = 4; Inclusion factor = 0.3; Acceptance error ratio = 0.1; A (random number) = 5; B = 6 (random number); N = 30030; (N = p1*p2 ,..., *pr = 2×3×5×7×11×13 = 30030); e (Public key) = 7, d (Secret key) = 823

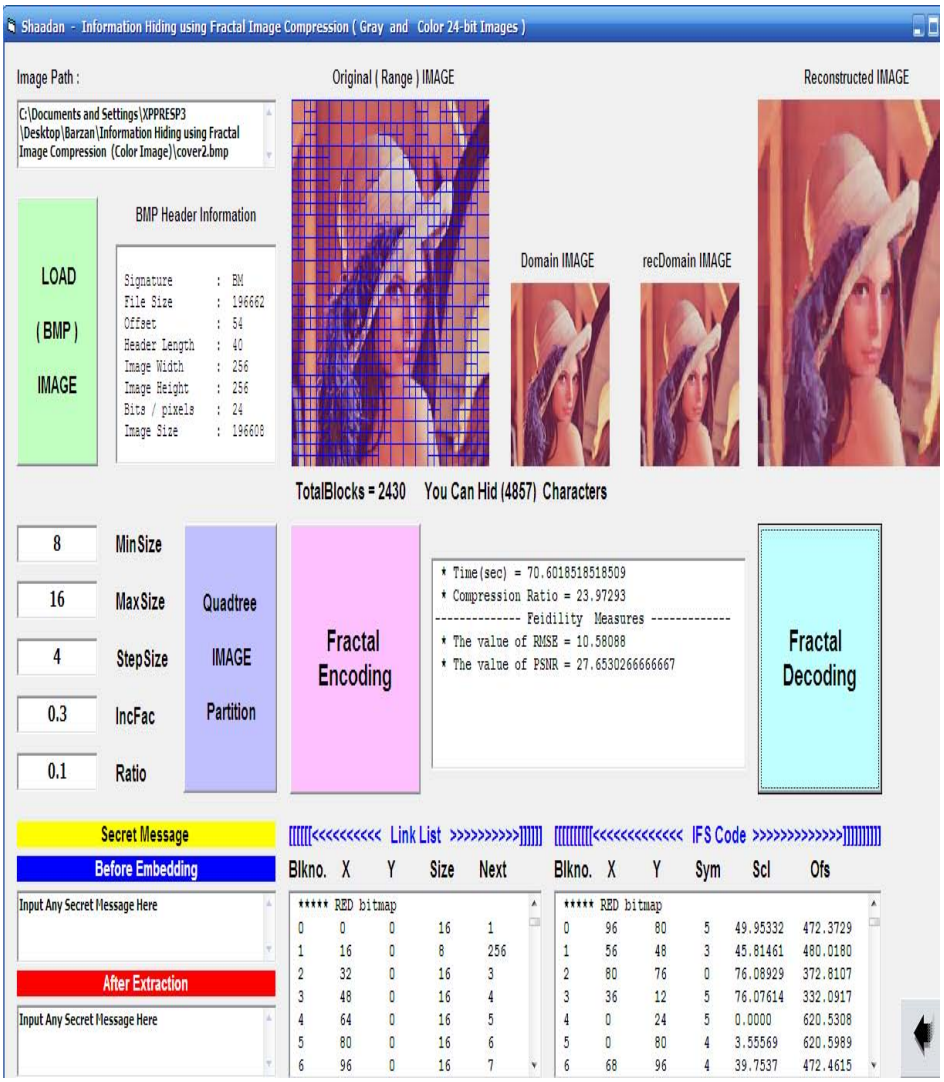

Fig. 5: Secret message extraction

CONCLUSION

During the implementation and testing phases of the proposed hiding system and cryptography the following remarks have been addressed: steganography is a technique not replace cipher system but rather to supplement it. If a message is encoded and hidden with a steganography method it provides an additional layer of protection and reduces the chance of the hidden message being detected.

RECOMMENDATIONS

In this study, various modifications based on modified RSA depended on multi-prime with Diffe-Hellman algorithm which is very secure and the quaidtree image partition with fractal transformation technique is very hard to detect in image steganography. It provides a better security for the sharing of data storage across networks. Important files carrying confidential information can be stored in the server in an encrypted form. No intruder can get any useful information from the original file during transmit media.

REFERENCES

Anderson, R.J. and F.A. Petitcolas, 1998. On the limits of steganography. IEEE J. Selected Areas Commun., 16: 474-481.

Cheng, H.D., X.H. Jiang, Y. Sun and J. Wang, 2001. Color image segmentation: Advances and prospects. Pattern Recognition, 34: 2259-2281.

Fisher, Y., 1995. Fractal Image Compression: Theory and Application. Springer, New York, USA., ISBN:9780387942117, Pages: 341.

Juneja, M. and P.S. Sandhu, 2013. Data hiding with enhanced LSB steganography and cryptography for RGB color images. Proceedings of the 2nd International Conference on Latest Computational Technologies (ICLCT'13), June 17-18, 2013, ICLCT, London, UK., pp: 1-4.

Kaur, S. and S. Kaur, 2017. Fractal image compression using quad tree decomposition and modified huffman coding. Imperial J. Interdiscip. Res., 3: 1332-1336.

Keerthika, S., 2017. Quality images using advanced fractal image compression method. Intl. Adv. Res. J. Sci. Eng. Technol., 4: 90-94.

Schettini, R., 1993. A segmentation algorithm for color images. Pattern Recognit. Lett., 14: 499-506.

Shanyu, T. and H. Yongfeng, 2011. Prediction of distortion pat-terns in image steganography by means of fractal computing. Proceedings of the 3rd International Conferences on Pervasive Pat-terns and Applications, September 25-30, 2011, International Academy, Research and Industry Association, Rome, Italy, pp: 128-132.

Shereek, B.M., Z. Muda and S. Yasin, 2014. Improve cloud computing security using rsa encryption withfermat's little theorem. IOSR J. Eng., 4: 1-8.